Lutte contre le crime et /ou vie privée

Poullet, Yves

Published in:
Terminal

Publication date:
2003

Document Version
le PDF de l'éditeur

Lutte contre le crime et/ou vie privée : un débat difficile !

À propos de l'alinéa 1er du paragraphe 2 de l'article 109 *ter* de la loi belge du 25 mars 1991 introduit par la loi belge du 28 novembre 2000 sur la criminalité informatique.

Yves Poullet*

> "Si tu es prêt à sacrifier un peu de liberté pour te sentir en sécurité, tu ne mérites ni l'une ni l'autre."
>
> Benjamin Franklin, Président des États-Unis.

L'histoire de l'article de loi portant réforme de certaines entreprises publiques témoigne de la légitimité de cette crainte et la consécration dans la loi récente sur la criminalité informatique des prestataires de la société de l'information avec les autorités policières ajoute, dans le contexte présent, celui des suites des attentats des tours du World Trade Center à cette angoisse d'un monde sécuritaire. La disposition belge n'est-elle pas évoquée dans les débats européens comme un modèle ?

Notre propos est dès lors de t'en offrir un commentaire en même temps que de prendre parti dans ce débat. Certains accents te rappelleront ceux des "avis" qu'en la matière la Commission nous a demandé bien souvent de commettre ensemble et dont la rédaction nous trouvait sur la même longueur d'onde.

La disposition nouvelle astreint sous peine de sanctions pénales les opérateurs de réseaux et les fournisseurs de services de télécommunications à conserver dans les limites du territoire de l'Union européenne, pendant une durée minimale de douze mois, les données d'appel des moyens de télécommunications et d'identification des utilisateurs de services. On ajoute qu'un arrêté royal délibéré en Conseil des ministres après avis de la Commission pour la protection de la vie privée déterminera le délai et les données à conserver. Cet arrêté royal n'a point encore été pris.

L'examen de cette disposition suit la démarche suivante :

- le premier point conduit à une description analytique de la portée du texte : qu'entend-on par "opérateurs" ou "fournisseurs de services" ? Quelles "données" peuvent ou doivent être conservées ?

* Doyen de la faculté de droit des FUNDP de Namur ; directeur du centre de recherche Informatique et Droit de Namur (http://www.crid.ac.be) ; yves.poullet@fundp.ac.be.

- le deuxième point évoque le débat européen actuel relatif à la lutte contre la cybercriminalité, débat ravivé par les suites des attentats du 11 septembre, en particulier les discussions du projet de directive sur la vie privée et le secteur des communications électroniques ;
- le troisième point, enfin, critique la disposition légale, objet de l'étude, du point de vue des principes de la protection de la vie privée contenus dans les textes tant internationaux, européens que belges.

La signification de la disposition

La disposition légale complète un texte récemment introduit. La loi du 11 juin 1998 modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées avait en effet introduit l'obligation de certains prestataires de services de communications de collaborer avec les autorités judiciaires. Selon la loi, le Roi détermine, après avis de la Commission de la protection de la vie privée, par arrêté délibéré en Conseil des ministres, "les moyens techniques par lesquels les opérateurs de réseaux et les fournisseurs de services doivent permettre le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement de télécommunications privées".

La crainte principale exprimée par la Commission de protection de la vie privée à l'égard de cette loi était le risque de l'instauration d'une surveillance exploratoire générale : sous réserve des limites que pourrait introduire l'arrêté royal, les autorités judiciaires reçoivent en effet le droit d'extraire des banques de données tenues par les opérateurs et fournisseurs de services des informations permettant une surveillance générale et exploratoire. Cette surveillance générale exploratoire est bannie par les principes établis par la Cour européenne des droits de l'Homme sur base de l'article 8 de la Convention européenne.

Le complément que la loi du 28 novembre 2000 ajoute à l'alinéa 1er du § 2 amplifie considérablement les moyens donnés à l'autorité policière puisqu'il s'agit de lui permettre d'accéder aux données de communication non seulement en temps réel mais également en temps différé. En effet, est mise à charge des prestataires de services de télécommunications l'obligation, sanctionnée pénalement, de mettre à disposition des autorités les données conservées sur le territoire de l'Union européenne, et ce pendant au "minimum" douze mois[1].

La disposition vise tout "opérateur et fournisseur de services de

1. Le délai de conservation a été fixé à "au minimum de douze mois" en dernière minute. La première proposition de loi laissait le soin au Roi de fixer ce délai. La Commission avait jugé dans son avis qu'il était nécessaire que le législateur se prononce lui-même sur cette durée vu l'impact de cette disposition sur nos libertés individuelles. La Commission de protection de la vie privée avait plaidé pour un délai plus court : trois mois comme le préconisent la loi allemande et la recommandation n° 3/99 relative à la conservation des données relatives aux communications pour les offreurs de service Internet en vue d'assurer le respect de la loi du "Groupe de protection des données" institué par l'article 29 de la directive 95/46/CE.

télécommunications". Par opérateurs de réseaux, on entend tout prestataire offrant des services traditionnels de transport et d'acheminement des messages, qu'ils s'agisse de réseaux publics ou privés comme des intranets propres à une administration ou à toute organisation, qu'il s'agisse de réseaux de mobilophonie, hertziens, satellitaires, câbles ou autres.

La notion de "fournisseur de services de communications" élargit encore le champ d'application de la disposition. On songe aux multiples prestataires intervenant dans l'offre de services de l'Internet (services d'accès, services de messagerie, *search engines*, portails, services de forum de discussion, etc.) ou dans l'offre de services à valeur ajoutée (services de cryptographie, services de *trusted third parties*, services électroniques bancaires...). On ajoute même les tenanciers de "cybercafés", les serveurs d'anonymisation, etc.

C'est à l'arrêté royal prévu par la loi de déterminer parmi cette liste ceux visés par la disposition légale. On notera que la plupart des "opérateurs" ou "fournisseurs" n'ont *a priori* aucune raison de conserver les données au-delà de la durée de connexion[2]. Nombre de ces services sont en effet gratuits. En d'autres termes, la seule finalité de la conservation des données est la manifestation de la vérité dans le contexte de la poursuite d'infractions. Cette contestation a des conséquences sur le fondement de la légitimité des traitements et bien évidemment sur le statut des personnes tenues à cette conservation.

Les données à conserver seront fixées également par arrêté royal. Il s'agit, selon le dispositif légal, des données d'appel des moyens de télécommunication[3] et des données d'identification des utilisateurs des services.

La liste de telles données est infinie. Le "*discussion paper*" préparé par les services de la Commission pour la réunion d'experts du 6 novembre relative à la rétention des données relève plus de 60 données susceptibles d'être ainsi collectées et conservées[4]. On notera en effet, à la suite de J.-M.

2. À cet égard, la remarque de la Commission de protection de la vie privée, o.c., p.9.
3. L'exposé des motifs (Doc. Parl., Chambre 0213/001, p. 30) précise qu'il s'agira notamment des données relatives à l'origine, la destination, la durée et la localisation des appels. Le Sénat (Doc. Parl., 2-392/3, p. 31) estime qu'ainsi les adresses IP des ordinateurs émetteurs et destinataires des télécommunications électroniques, les log-in et les log-out, l'heure et début de la fin de connexion voire les adresses Internet visitées font partie des données d'appel.
4. L'annexe 2 du *discussion paper* (29 octobre 2001) préparé par les services de la Commission dans le cadre du EU Forum on Cybercrime du 27 novembre 2001 et de la réunion d'experts préparatoire du 6 novembre établit la longue liste des types de données susceptibles d'être enregistrées et ce par types de service Internet : ainsi, pour l'e-mail server : SMTP log ; date and time of connection of client to server; IP adress of sending computer ; message ID ; sender e-mail adress; receiver e-mail adress ; status indicator ; POP log or IMAG log ; date and Time of connection of client connected to server ; IP adress ; User ID ; (in some cases) identifying information of e-mail retrieved ; File upload and download servers ; pour le FTP (file transfer protocol) log, date and time of connection ; IP source adress ; path and filename of Data object uploaded or downloaded ; pour les services web : Http log ; date and time of connection ; IP source adress ; operations (types of command) ; path of operation ; last visited page ; Response codes ; ....

Dinant, d'une part, que ces traces se multiplient du fait de l'utilisation de plus en plus généralisée des services de communication dans tous les secteurs de la vie professionnelle et non professionnelle et, d'autre part, que les détenteurs, la nature et le lieu du stockage de ces traces deviennent de moins en moins visibles par l'individu qui les crée et les abandonne au gré des réseaux le plus souvent malgré lui.

Ainsi, lors d'une visite d'un site Web proposé par un serveur quelconque et ce à partir du site d'une société fournisseur d'un service d'indexation automatique (*search engines*) comme Lycos Altavista, l'internaute laissera, sans compter les nombreux traitements invisibles possibles, des traces chez le ou les opérateur(s) des réseaux de télécommunications que son message empruntera, chez le fournisseur d'accès et chez les différents serveurs des sites visités. La nature des traces laissées dans l'exemple donné est variée. Si l'opérateur de réseau garde les traces du trafic (le numéro appelant ou plutôt l'adresse du destinataire du message), le fournisseur d'accès peut dans son *logbook* conserver la trace des diverses utilisations opérées à partir du système d'information de l'internaute : les différents sites visités, voire les pages visitées et le parcours suivi, la durée de chaque visite et bien évidemment les caractéristiques de la configuration utilisée par l'internaute. Une même richesse d'informations se retrouvera chez l'opérateur du service de recherche et d'indexation automatique, voire chez la société de cybermarketing avec laquelle le "*search engine*" sera connecté par un hyperlien invisible.

Les textes européens, ceux du projet de directive et de la convention européenne du Conseil de l'Europe, distinguent au sein de ces données, quelques catégories. Ainsi, le Conseil de l'Europe distingue les "données relatives au trafic" et celles "relatives à l'abonné" ; le projet de l'Union européenne, celles de trafic et celles de localisation. Nous reviendrons sur l'intérêt de telles distinctions.

Les débats européens relatifs à l'obligation de conservation des données de trafic

Deux enceintes européennes discutent ou achèvent leurs discussions sur l'obligation de conservation des données de communication et son corollaire : l'obligation de collaboration entre les instances privées chargées de cette conservation et les instances publiques, autorités judiciaires ou policières.

Le Conseil de l'Europe

Le Conseil de l'Europe a adopté le 8 novembre 2001 le premier traité international contre la "cybercriminalité". Il l'ouvrait à la signature des États membres ou non[5], le 23 novembre à l'occasion de la conférence de Budapest.

5. Ainsi, les États-Unis, non membres du Conseil de l'Europe, ont signé la Convention le jour même de l'ouverture de celle-ci à la signature des États.

Le texte fait suite à la recommandation n° R(95)13 du Comité des ministres relative aux problèmes de procédure pénale liés à la technologie de l'information[6]. Il est le fruit des travaux d'un comité créé dès 1997 chargé d'élaborer une convention sur la cybercriminalité dans le cyberespace et de renforcer ainsi la coopération internationale.

La recommandation se limitait à prescrire des "obligations spécifiques [...] pour les fournisseurs de services qui offrent des services de télécommunications au public *via* des réseaux de communication publics ou privés, de délivrer l'information nécessaire, lorsque les autorités compétentes chargées de l'enquête l'ordonnent, pour identifier l'utilisateur". Il s'agissait donc essentiellement dans le cas d'une enquête de permettre aux autorités policières de réclamer l'identité d'un abonné ou d'un client et ce, à partir d'une adresse TCP/IP ou d'un numéro téléphonique ou de mobilophone. La convention de 2001 contient diverses obligations pour les États signataires, étant entendu, rappelle l'article 15, que la mise en œuvre des règles prévues doit être soumise "aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'Homme et des Libertés". Ce principe général induit clairement le devoir d'un respect de l'article 8 de la Convention européenne des droits de l'Homme et de la jurisprudence qui l'a suivi et interprété.

La première obligation concerne la conservation "rapide" (expéditions) de données spécifiques y compris des données de trafic qui ont été stockées aux moyens d'un système informatique. Elle incombe aux personnes gardiennes de ces données (*in the person's possession or control*) et l'article 16 prévoit que cette conservation rapide a une durée maximale de quatre-vingt-dix jours[7] éventuellement renouvelable. Cette disposition est loin d'avoir la portée générale de la disposition belge. Elle vise dans le cadre d'une enquête relative à une infraction déterminée le droit des autorités de demander à une personne déjà en possession de certaines données de les conserver pour éviter leur disparition. Elle n'autorise pas l'État à réclamer des opérateurs ou fournisseurs des devoirs supplémentaires de collecte de données et surtout pas à opérer cette conservation vis-à-vis de toutes les utilisations de son ou ses services[8].

L'article 17 souligne que la conservation et la divulgation des données conservées sur base de l'article 16 se conçoit d'un nombre suffisant de données de trafic de manière à permettre "l'identification des fournisseurs de services et de la voie par laquelle la communication a été transmise".

À côté de ce premier prescrit, l'article 18 de la convention crée l'obligation pour les États membres d'introduire des dispositions permettant aux autorités compétentes d'ordonner "à un fournisseur de

6. Disponible à http://www.coe.fr/cm/ta/rec/1995/f95r13.htm.
7. La durée de conservation d'un an avait été prévue. Elle a été sévèrement réduite à la suite de la pression des autorités de contrôle en matière de protection des données et des associations de défense des libertés.
8. Il est à noter que le Parlement européen dans son avis du 6 septembre 2001 avait insisté sur le fait qu'"il ne doit pas être établi de principe général de conservation".

service de communiquer les données relatives à l'abonné qui sont en possession ou sous le contrôle de ce fournisseur de services". L'article 18 prévoit que par "données relatives aux abonnés" il faut entendre exclusivement les données portant "sur l'identification des personnes utilisatrices des services fournis par les opérateurs et sur les caractéristiques techniques des services fournis par les opérateurs et sur les caractéristiques techniques des communications assurées par ces derniers. Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultables sous quelque forme que ce soit, dans le cadre de ces communications".

On notera que le devoir de production ainsi prévu ne concerne que des données déjà traitées par le fournisseur de service dans le cadre normal de ses activités et ne vise que les données dites de connexion, c'est-à-dire les données relatives à l'identité des personnes qui se connectent au service à l'exclusion des données dites de trafic, ainsi la liste des sites visités, la durée de connexion, etc.

Cette exclusion des données quant à l'utilisation du service est le fruit de longs débats et en particulier des oppositions marquées d'une série d'associations américaines et européennes de défense des libertés[9] de même que du Groupe européen de protection des personnes à l'égard du traitement des données à caractère personnel dit "groupe de l'article 29[10]".

L' Union européenne

La position européenne, qui a toujours privilégié l'approche "protection des libertés", s'est trouvée singulièrement mise en cause, à la suite des attentats du 11 septembre sur le sol américain.

La réaction de nombreuses instances européennes à la découverte du réseau d'écoutes appelé Echelon illustre particulièrement bien la première approche européenne. Ce réseau, géré principalement par les États-Unis, permet aux services d'intercepter et d'analyser les messages ou certains messages transitant par satellites, qu'il s'agisse de communications téléphoniques ou électroniques. Certes, les réactions furent lentes à venir depuis le rapport STOA de 1998[11] et ce en raison de la participation du Royaume-Uni au réseau Echelon, de la présence de bases d'écoutes en Allemagne et en Angleterre et finalement de l'existence d'un réseau français concurrent. Elles devraient cependant aboutir, grâce notamment à l'intervention du groupe européen de protection des données, à une résolution votée par le Parlement européen le 5 septembre 2001 dans la foulée du rapport Schmidt. On y lit notamment parmi les considérants, une

9. Ainsi, on soulignera le rôle joué par l'EPIC (U.S.), le Privacy International (UK) et l'Electronic Frontier Foundation.

10. À cet égard, de manière très nette, la Recommandation 2/99 concernant le respect de la vie privée dans le contexte de l'interception des télécommunications adoptée le 3 mai 1999 (WP 18, 5005 99/final).

11. *Cf.* le rapport "Une évaluation des techniques de contrôle politique", septembre 1998, et plusieurs études, avril et mai 1999, publiées par le STOA (*Scientific and Technological Options Assessment*) du Parlement européen.

condamnation des pratiques d'interception non conformes aux principes de la convention européenne des droits de l'Homme.

La volonté européenne de protéger, en vertu du principe de souveraineté, la vie privée des citoyens européens se heurte cependant à des impératifs de sécurité et en particulier de lutte contre la cybercriminalité. Depuis le traité d'Amsterdam, l'Europe est en effet compétente à prendre des initiatives fondées sur le 3e pilier. Cette nécessité d'un équilibre est affirmée par une communication de la Commission en date du 26 janvier 2001 : "La présente communication s'interroge sur la nécessité d'une initiative en vue de définir une politique globale et étudie les différentes formes qu'elle pourrait prendre, dans le contexte des objectifs plus larges que constituent la société de l'information et la création d'un espace de liberté, de sécurité et de justice, en vue d'améliorer la sécurité des infrastructures de l'information et de lutter contre la criminalité informatique, dans le respect des droits fondamentaux de la personne, conformément à l'engagement pris par l'Union européenne."

Appliquant le principe d'une balance à l'obligation de stockage de certaines données de trafic, la communication distinguait celles traitées par les opérateurs et fournisseurs de services dans le cadre normal de leurs activités de facturation[12] et celles qui obligeraient les opérateurs et les fournisseurs de service à traiter des données aux seules fins d'enquêtes pénales. À l'égard des premiers, la Commission estime que les États membres peuvent adopter des mesures législatives visant à limiter la portée de cette obligation d'effacement des données relatives au trafic lorsqu'une telle limitation constitue une mesure nécessaire, entre autres, pour la prévention, la recherche, la détection et la poursuite d'infractions pénales ou pour l'utilisation non autorisée du système de télécommunications[13].

12. Conformément aux directives communautaires sur la protection des données à caractère personnel, et plus précisément au principe général de limitation des transferts à une finalité spécifique énoncé dans la directive 95/46/CE et aux dispositions particulières contenues dans la directive 97/66/CE, les données relatives au trafic doivent être effacées ou rendues anonymes dès que le service de télécommunications a été fourni, sauf lorsqu'elles sont nécessaires à des fins de facturation. Dans le cas d'un accès forfaitaire ou gratuit aux services de télécommunications, les fournisseurs de services ne sont pas autorisés, en principe, à conserver les données relatives au trafic.
13. La Communication précise, se faisant d'ailleurs l'écho des dispositions de l'article 14 de la directive 97/66/CE et de l'article 13 de la directive 95/16/CE : "Cependant toute mesure législative prise à l'échelon national qui prévoirait la conservation des données relatives au trafic pour les besoins de l'application des lois devrait remplir certaines conditions. Les mesures proposées devraient en effet être appropriées, nécessaires et proportionnées au but poursuivi, comme le prévoient le droit communautaire et le droit international, notamment la directive 97/66/CE et la directive 95/46/CE, la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 et la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Le respect de ces conditions et de ces principes serait d'autant plus important pour les mesures qui impliquent la conservation systématique des données sur une large fraction de la population."

Vis-à-vis du second type de données, la Commission énonce que leur enregistrement et leur conservation ne peuvent se justifier que pour des raisons exceptionnelles et pour une durée très limitée.

À cet égard, elle évoque la résolution du Parlement européen qui, dans une matière très particulière, la lutte contre la pornographie enfantine, a admis à titre tout à fait exceptionnel la conservation des données relatives au trafic pendant une durée de trois mois.

Les attentats du 11 septembre et la demande insistante de l'administration américaine d'une meilleure collaboration des États européens à la lutte contre le terrorisme supposent de revoir les mécanismes de protection des données informatiques de manière à assurer une lutte efficace contre les réseaux terroristes opérant notamment via les réseaux modernes de communication[14].

On notera que dans un temps record, "*with all the urgency of a nation at war*", la Maison-Blanche avait fait adopter par le Congrès un certain nombre de textes législatifs pour permettre une lutte efficace contre la terrorisme, en particulier le *Patriot Act*[15], dont certaines dispositions concernent les écoutes téléphoniques[16]. On notera que les dispositions américaines ne prévoient pas d'obligation de stockage des données de trafic pour les prestataires de service de communications au-delà de ceux nécessités par les services offerts par ces derniers[17] ; que la communication de telles données conservées n'est pas imposée mais se fait sur une base volontaire dans le cadre de "*codes of conduct*" élaborés entre ces prestataires et les autorités judiciaires ou de sécurité ; enfin que les obligations de communiquer les données de trafic sont entourées de nombre de garanties procédurales et de sanctions pénales et civiles en cas de non-respect des conditions légales imposées par le texte légal[18] et ne peuvent en aucune manière donner lieu à un accès au contenu des communications[19].

14. *Cf.* notamment les articles publiés par les journaux en octobre à la suite des discussions entre le président Bush et le premier ministre belge, la Belgique assumant alors la présidence de l'Union européenne, ainsi, notamment, *la Libre Belgique* du 22 octobre 2001; *Gazet van Antwerpen* du 26 octobre 2001.
15. "*Uniting and Strenghtening America by providing Appropriate Tools Required to Intercept and Obstruct Terrorism*"(USA patriot act), Act of 2001, HR 3162, 1st Session, 107 th Congress, disponible sur le site http://thomas.loc.gov, approuvé par le Sénat le 25 octobre et signé par le président Bush le 26 octobre.
16. À cet égard, on notera les déclarations de Bush après l'adoption de cette loi, lors de la signature présidentielle de la loi : "*This law will give intelligence and law enforcement officials new tools to fight a present danger... to counter a threat like no other our nation has ever faced.*"
17. Sect. 222 : "*Nothing in this Act shall impose any additional technical obligation or requirement on a provider of a wire or electronic communication service or other person to furnish facilities or technical assistance...*"
18. Sect. 223 : "*Civil Liability for certain unauthorized disclosure*".
19. Sect. 212 insérant notamment un § 2703 "*Required disclosure of customer communications or records*" : "*A provider of electronic communications service or remote computing service shall disclose a record or other information pertaining to a subscriber or to a customer of such service (not including the contents of communications covered ...) to a governmental entity.*"

Enfin, sous la pression des *lobbies* des défenseurs des libertés, la loi prévoit une clause de "Sunset"[20], qui limite à quatre ans la durée de vie des dispositions légales.

La discussion entamée dès 2000 de la révision de la directive 97/66 concernant le traitement des données à caractère personnel et la protection des données dans le secteur des télécommunications[21] devait fournir le cadre principal de cette réponse européenne à la demande américaine. Cette proposition de directive était à l'origine intégrée dans un ensemble de propositions visant à réformer la réglementation des télécommunications européennes afin de l'adapter aux développements technologiques et du marché des services des télécommunications. La proposition devenue projet est aujourd'hui l'objet d'une "position commune arrêtée par le Conseil en vue de l'adoption de la directive"[22]. La proposition initiale énonçait le principe suivant lequel les données de trafic et de localisation ne pouvaient être conservées et utilisées, sauf consentement exprès du client dans le cadre de l'offre de services à valeur ajoutée, qu'aux fins de facturation et d'interconnexion. Cette proposition initiale reprenait la solution déjà affirmée par la directive 97/66. Lors des discussions qui ont précédé les événements dramatiques du 11 septembre, le Conseil des ministres des Télécommunications du 27 juin avait déjà été sensible[23] aux demandes venant de certaines autorités policières en acceptant l'ajout d'une phrase au considérant n° 10 du préambule[24] : "Cette directive n'affecte pas le droit des États membres de mener des interceptions légitimes de communications électroniques ou de prendre d'autres mesures telles que d'ordonner la conservation des données de trafic ou de localisation pour une période limitée quand cette conservation est nécessaire et justifiée pour ces raisons et en conformité avec les principes généraux du droit communautaire".

Les suites des attentats provoquèrent des discussions importantes en la matière. Le 20 septembre, la réunion des ministres européens de la Justice et des Affaires intérieures adopte des conclusions qui requièrent que tous les fournisseurs de télécommunications conservent les données et y donnent accès aux autorités policières "à des fins d'enquêtes criminelles"

---

20. Sect. 224 à propos de ces mesures qui assurent selon le sénateur T. Dashle, "*an appropriate balance between protecting civil liberties, privacy and ensuring that law enforcement has the tools to do what it must*" : "*Negotiators have placed safeguards on the legislation, like a four-year expiration date on the wiretapping and electronic surveillance portion, court permission before snooping into suspects' formerly private educational records and court oversights over the FBI's use of a powerful e-mail wiretap system*". J.J. Holland, *Senate sends Antiterrorism Legislation to Bush*, texte disponible à : http://www.washingtonpost.com /wp-dyn/articles/A51682-2001Oct25.html.
21. JO, L. 24 du 30.1.1998, p. 1.
22. La position commune a été adoptée par le Conseil, le 21 janvier 2002 (Dossier institutionnel 2000/0189 (COD), 15396/01).
23. ... sous la pression des gouvernements français et anglais.
24. La Commission par la voix de son commissaire E. Liikanen avait insisté sur le fait qu'une telle clause ne pouvait avoir que le statut d'un "*Recital*" et ne devait pas être incluse dans le texte de la convention.

et réclame de la Commission européenne la révision de la législation européenne de manière à garantir une contribution aux efforts des autorités en charge de l'application des lois pénales.

Pour répondre à cette demande relayée aussitôt par les autorités policières, la Commission organisa le 27 novembre 2001 un "*hearing*" à Bruxelles sur le cybercrime[25]. Cette réunion fut précédée d'une réunion d'experts le 6 novembre ayant pour objet unique la conservation des données de trafic[26] rassemblant des représentants des autorités de protection des données, des autorités policières et de l'industrie. Il ressort de ces discussions menées à la fois lors de la réunion d'experts et lors de l'audition du 27 novembre :

- du côté de l'industrie, un double point de vue : celui des fournisseurs de services de télécommunication[27] de pouvoir opérer une conservation des données à des fins de sécurité de leurs propres systèmes d'information et des mêmes personnes leur malaise de devoir collaborer "gratuitement" à des demandes d'autorités bien souvent mal libellées ou vagues ; celui des ayants droit des titulaires de droit d'auteur d'utiliser les compétences policières qui pourraient être reconnues pour mieux lutter contre la cybercriminalité que constitue le copiage illicite d'œuvres sur le réseau ;
- celui des autorités de protection des données[28] de s'opposer à la

25. Un premier *hearing* avait été organisé le 7 mars 2001 à propos de sa communication sur le cybercrime de manière à permettre aux représentants de chaque catégorie d'intérêts (opérateurs de réseaux ; fournisseurs de service ; autorités policières ; autorités de protection des données ; association de libertés) de faire valoir leur point de vue.
26. À propos de cette réunion, *cf.* le *discussion paper* préparé par les services de la Commission et disponible sur le site de la Commission à l'adresse : http://europa.eu.int/information_society/topics/telecoms/internet/crime/wpapnov/index.htm.
27. *Cf.* en particulier la position d'AOL : "*AOL retains only data that is necessary either for billing purposes, fraud prevention or security.*" "*AOL cannot cost a potential data retention obligation without understanding fully what would be required from us. However, some costs consideration would be, not only the storing of data but more importantly the cost of keeping the integrity of the data and the costs associated with data retrieval.*" Cf. également la position de l'European Association of Consumers Electronic Manufacturers (EICTA) et de l'EACEM, qui estiment que l'obligation de conservation de données impose des charges financières importantes aux fournisseurs de service et s'opposent à toute conservation obligatoire des données de trafic sauf dans le cas de poursuites relatives à des infractions déterminées : "*Under a data preservation order, service providers store data related to a particular person, rather than store all users' data for potential future investigations. Bescause data preservation requirements are directed at particular person or persons, they do not pose the same privacy concerns as general data retention.*"
28. À ce propos, l'intervention de P. Schaar à la réunion d'experts du 6 novembre 2001 et celle de D. Smith au Hearing du 27 novembre. On se référera en outre aux "opinions" émises par le Groupe de protection des données de l'article 29, en particulier, la dernière (5074 final) adoptée le 5 novembre 2001 à propos de la communication de la Commission : "*Creating a safer information Society by improving the security of information infrastructures and combating computer-related crime*" (disponible à http://europa.eu.int/commm/internal_market/en/dataprot/wpdocs/index.htm), et aux travaux de l'International Working Group on Data Protection in Telecommunications, *Common Position on Data Protection aspects, in the Draft Convention of Cybercrime* of the Council of Europe, 13-14 sept. 2000, texte disponible à l'adresse : http://www.datenschutz-berlin.de/doc/int/iwgdpt/cv_en.htm.

conservation des données au-delà des strictes nécessités de la facturation et de manière plus générale de définir des mesures procédurales de telle manière qu'elles soient en parfaite conformité avec les droits fondamentaux et les libertés des citoyens et avec les législations de protection des données : ainsi, les commissaires à la protection des données rappellent l'interdiction de toute mesure générale de surveillance et la nécessité de justification concrète pour la rétention de données de trafic spécifiées. Enfin, "la durée de rétention des données et le nombre de données doivent être en proportion avec la gravité de l'infraction criminelle". Enfin, les autorités de protection des données soulignent le caractère très sensible des données de trafic, qui révèlent le comportement d'un individu dans la mesure de la généralisation croissante de l'utilisation des moyens de télécommunications dans la vie courante ;

- celui des autorités policières qui considèrent comme vitale la possibilité pour la police de résoudre des cas grâce à la conservation des données de trafic et de localisation et à la collaboration convenue ou imposée par la loi des fournisseurs de services de télécommunications. Ces autorités soulignent que cette nécessité est absolue pour certains types d'infraction[29] dans la mesure où, sans cette conservation et collaboration, il leur serait impossible de détecter les criminels. Enfin, les autorités policières justifient la longue liste des données de trafic à conserver et les durées de conservation (entre six mois et deux ans).

Les autorités européennes devaient tirer les conclusions de ces débats en modifiant légèrement le texte de la proposition de directive. Ainsi, la position commune à laquelle nous avons déjà fait référence élargit les finalités légitimes pour lesquelles les fournisseurs de réseaux ou de services de télécommunications peuvent traiter les données de trafic ou de localisation. L'article 6.5 ajoute au texte initial la finalité de détection des fraudes et le traitement en vue de la commercialisation de services à valeur ajoutée n'est plus soumis au consentement de la personne concernée. Surtout, l'article 15 autorise les États membres à "adopter des mesures législatives visant à limiter les droits et obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la sécurité nationale –c'est-à-dire la sûreté de l'État– la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE". À cette fin, ajoute le texte, "les États membres peuvent, entre autres, prévoir la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe, dans le respect des principes généraux du droit communautaire"[30].

29. *Cf.* en particulier l'audition de l'autorité policière norvégienne qui relève en particulier les infractions suivantes : "*breaking into computer systems ; theft of trade secrets ; sabotage of critical IT systems ; abuse of telephone systems ; fraud ;threats of life and health ; blackmail ; harassement and defamation...*"

30. Le considérant n° 11 note que "lesdites mesures doivent être appropriées, rigoureusement proportionnées au but poursuivi et nécessaires dans une société démocratique".

Le texte ainsi revu laisse chaque État libre de procéder comme il le souhaite. En ce sens, il ne répond pas aux objections des fournisseurs de services, inquiets des différences d'interprétation que pourrait donner chaque État membre à une disposition aussi floue quant à la durée de conservation, quant aux données à conserver et quant aux modalités de cette conservation ; elle heurte les principes de protection des données tels que les autorités de protection des données les avaient interprétés ; enfin, tout en leur donnant raison sur le principe de la conservation des données, elle renvoie les juges et policiers à leurs gouvernements nationaux pour obtenir une légalisation nationale de l'obligation de conservation et de collaboration des fournisseurs d'infrastructure et de services. On note que dès le 31 octobre, le législateur français devait, dans le cadre de la loi sur la sécurité quotidienne[31], traduire cette compétence laissée aux législateurs nationaux en des textes sur la teneur desquels nous reviendrons dans l'analyse critique.

Analyse critique – Pistes pour le suivi de l'obligation légale de conservation des données et de collaboration des fournisseurs de services de télécommunications.

Les compléments du paragraphe 2 de l'article 109 *ter* E apportés par la loi sur la criminalité informatique apparaissent donc comme une transcription anticipée d'une directive en voie d'approbation. Notre souci est dans ce dernier point de proposer quelques réflexions qui puissent servir de guide à la réglementation qui donnera à la loi sa pleine efficacité en même temps que nous reviendrons sur les choix opérés par nos législateurs.

Notre première réflexion est liminaire. Elle souligne l'importance des données dont il est question lorsqu'on parle des données de localisation ou de trafic. La notion de données de trafic est définie par le législateur européen comme "toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation", et celle de "données de localisation" comme "toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public". De telles données sont infinies : elles comprennent, outre les données de simple connexion, leur durée, les destinataires de nos messages, les sites visités, la longueur des messages échangés, les caractéristiques du message et du système d'information de l'utilisateur ; les données de localisation révèlent à quelques mètres près l'endroit où se trouve un mobilophone ou un GPS même non en cours d'utilisation. C'est que l'utilisation de plus en plus intensive des technologies de l'information et la multiplication de services à valeur ajoutée qui leur sont attachés trahissent

31. Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, JO du 16 novembre 2001.

les relations que nous nouons avec autrui ; de nos déplacements, de nos goûts, nos convictions voire nos maladies, elles laissent en effet chez des intervenants de plus en plus nombreux et divers, de plus en plus de traces en des lieux certes disparates mais susceptibles d'être reliés grâce aux vertus des réseaux et de systèmes de plus en plus performants de traitement de l'information.

Bref, la possibilité d'avoir accès à ces multiples fichiers et de pouvoir en croiser les données crée des possibilités bien tentantes pour l'autorité policière ou judiciaire. Au-delà, on s'interroge sur la possibilité de maintenir une distinction entre les données de trafic et celles de contenu. Cette distinction parfaitement claire lorsqu'il s'agissait des données relatives aux communications téléphoniques traditionnelles où les données relatives aux correspondants d'une communication et à leur localisation dans le temps et la durée, s'efface en effet lorsque, dans les réseaux modernes, la donnée dite de trafic révèle le contenu même de la communication, ainsi l'accès à une page Web voire à un site Web révèle le contenu de la communication.

Faut-il introduire dès lors des limites à ce stockage, des modalités particulières à cette opération et aux possibilités d'accès des autorités chargées de la poursuite des infractions ? On rappellera à cet égard, l'arrêt fondamental de la Cour européenne des droits de l'Homme, dit arrêt Klass du 6 septembre 1978, où la Cour reconnaît le pouvoir discrétionnaire des États quant au choix des systèmes de surveillance auxquels ils peuvent avoir recours, mais souligne que ce pouvoir discrétionnaire ne signifie pas un pouvoir arbitraire : "Consciente du danger inhérent à pareille loi de saper voire de détruire la démocratie au motif de la défendre, la Cour affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée..." La principale question qui se pose en l'occurrence sur le terrain de l'article 8 consiste à savoir si les termes du paragraphe 2 suffisent à justifier l'ingérence ainsi constatée. Ménageant une exception à un droit garanti par la Convention, ce paragraphe appelle une interprétation étroite. Caractéristique de l'État policier, le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire "à la sauvegarde des institutions démocratiques".

Le Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, dans sa recommandation 2/99 concernant le respect de la vie privée dans le contexte de l'interception des télécommunications[32], avait résumé les garanties à respecter découlant de la jurisprudence du Conseil de l'Europe en la matière[33]. "Il importe que le droit national, par des dispositions accessibles à tout citoyen, précise de

32. Recommandation adoptée le 3 mai 1999 (Doc. 5005/99/final, WP 18, déjà cité). Pour rappel, cette recommandation avait été émise dans le cadre des réactions européennes à la découverte du réseau Echelon (*Cf. supra*).

33. Sur cette jurisprudence, lire le remarquable article de YERNAULT D., "Echelon et l'Europe - La protection de la vie privée face à l'espionnage des télécommunications", *JTDE*, 2000, 190 et s.

façon rigoureuse et dans le respect de toutes les dispositions susmentionnées :

- les autorités habilitées à permettre l'interception légale des télécommunications, les services habilités à procéder aux interceptions et la base légale de leur intervention ;
- les finalités selon lesquelles de telles interceptions peuvent avoir lieu, qui permettent d'apprécier leur proportionnalité par rapport aux intérêts nationaux en jeu ;
- l'interdiction de toute surveillance exploratoire ou générale des télécommunications sur une grande échelle ;
- les circonstances et les conditions précises (par exemple éléments de fait justifiant la mesure, durée de la mesure) auxquelles sont soumises les interceptions, dans le respect du principe de spécificité dont relève toute ingérence dans la vie privée d'autrui ;
- le respect de ce principe de spécificité, corollaire de l'interdiction de toute surveillance exploratoire ou générale, implique en ce qui concerne plus précisément les données de trafic que les autorités ne peuvent avoir accès à ces données qu'au cas par cas, et non de façon générale et proactive ;
- les mesures de sécurité en ce qui concerne le traitement et le stockage des données, et leur durée de conservation ;
- en ce qui concerne les personnes impliquées de façon indirecte ou aléatoire dans les écoutes[34], les garanties particulières apportées au traitement de données à caractère personnel : notamment, les critères justifiant la conservation des données et les conditions de la communication à des tiers ;
- l'information de la personne surveillée, dès que possible ;
- les types de recours que peut exercer la personne surveillée ;
- les modalités de surveillance de ces services par une autorité de contrôle indépendante ;
- la publicité –par exemple sous forme de rapports statistiques réguliers[35]– de la politique d'interception des télécommunications effectivement pratiquée ;
- les conditions précises auxquelles les données peuvent être communiquées à des tiers dans le cadre d'accords bi ou multilatéraux.[36]

L'application de ces principes à des mesures qui vont au-delà de la simple interception de communications électroniques pour s'étendre à l'analyse de données de communications antérieures appelle nombre de commentaires. Le prescrit belge réclame de tous les fournisseurs et opérateurs de services de communication électronique le stockage de certaines données de communication sans différencier les personnes concernées. Il est difficile, au vu de tels prescrits, de ne pas parler de

34. ... ainsi la personne en lien avec la personne surveillée et sa localisation dans le cas d'un contact par téléphone mobile.
35. Il s'agit d'une exigence rappelée par le groupe dit de Berlin (Groupe international de travail sur la protection des données dans le secteur des télécommunications) adoptée lors de la réunion de Hong Kong le 15 avril 1998, recommandation sur la *"public accountability in relation to interception of private communications"*.
36. En particulier dans les réseaux européens de coopération policière et judiciaire comme Europol et Infopol voire, comme souhaité par les États-Unis, vers les autorités de défense américaines.

surveillance générale. Il y a lieu de craindre, comme le notait le député européen M. Cappato, rapporteur au Parlement dans le débat qui nous occupe, que le surveillé, l'"ennemi", ne devienne "le simple citoyen qui surfe sur le Net ou qui passe un coup de téléphone". Cette remarque critique sur la légitimité d'une telle mesure en induit d'autres. Une première consiste à distinguer les traitements, selon leur finalité originaire ; la deuxième s'interroge sur la proportionnalité des mesures prises vis-à-vis des risques censés justifier de telles mesures et la troisième s'interroge sur les risques créés par les traitements induits par le prescrit en cause.

Deux types de traitements

Le caractère général du prescrit belge ne distingue pas, à l'inverse de la loi française, les données collectées et conservées légitimement par les opérateurs et fournisseurs de service de communication dans le cadre de leurs propres activités, d'autres données dont la conservation n'est pas a priori requise dans le cadre de leurs activités. Le projet de directive européenne, nous l'avons vu, en dehors du consentement de la personne concernée, légitime la conservation des données pour deux finalités : celle de la facturation et de son paiement et celle de la sécurité du système d'information ou du réseau de cet opérateur et du fournisseur (repérage de tentatives de hacking, de sabotage, d'envoi de virus, etc.)[37].

Pour les données conservées et traitées dans le cadre de ces finalités, la communication de telles données aux autorités policières représente un traitement ultérieur au sens des législations de protection des données dont la compatibilité s'apprécie en fonction des principes suivants.

En ce qui concerne les données pour lesquelles aucune finalité légitime de conservation n'existe chez l'opérateur ou le fournisseur, la seule finalité légitime réside dans la poursuite d'infractions. En d'autres termes, dans ce second cas, c'est directement l'autorité publique qui est responsable du traitement qu'il confie à l'opérateur ou au fournisseur lui-même voire à un service autre, qui serait chargé de collecter les données provenant des différents opérateurs et fournisseurs. Ces fournisseurs, opérateurs ou services ne sont alors que des sous-traitants et l'article 16 de la directive qui soumet ces sous-traitants (et engagement de non-utilisation des données en dehors de la mission confiée) s'applique.

Dans ce cas, la légitimité de conservation ne peut se fonder que sur les fins d'investigation policière.

Nous sommes des États de droit et la Convention à laquelle nous adhérons impose que ceux qui réclament la conservation des données en

37. On rappelle que la première proposition de directive ne mentionnait pas cette finalité, introduite par la suite à la demande des opérateurs. On peut s'inquiéter du caractère vague de cette finalité nouvelle de conservation des données même s'il va de soi que les principes de l'article 6 de la directive dite générale de protection des données s'appliquent et obligent dès lors le fournisseur ou l'opérateur de services de communications à ne procéder à des traitements loyaux que pour des finalités déterminées et compatibles, qu'à propos de données pertinentes et adéquates par rapport à ces finalités et finalement que pour la durée strictement nécessaire.

démontrent l'intérêt social impérieux par rapport aux droits et libertés ainsi diminuées. Où sont de telles justifications ? Les autorités policières apparaissent bien muettes lorsque, interrogées à une réunion d'experts convoqués encore récemment par la Commission européenne pour préparer ce forum, elles s'avéraient incapables de présenter autre chose que des opinions, des faits divers là où des études statistiques, sociales et psychologiques auraient pu démontrer qu'effectivement la préparation active de crimes graves passe par l'utilisation de moyens de communication et qu'effectivement le travail d'investigation exige l'accès rapide aux données d'une telle utilisation. La confrontation avec les fournisseurs de services a, au contraire, révélé l'imprécision des demandes, leur tâtonnement et la rareté de l'efficacité de telles démarches.

Légitimité des traitements d'investigation policière

La légitimité des données repose sur un examen de proportionnalité : le risque d'atteinte à la sécurité de l'État, à la protection des individus justifie-t-il un traçage "tous azimuts" et ce moyen proposé est-il nécessaire à l'obtention de telles fins ?

À cet égard, la gravité du crime est évoquée pour justifier de telles atteintes. On s'interroge. Y a-t-il un lien fort et nécessaire entre le moyen mis à disposition de l'autorité policière et la découverte des délinquants ?[38] Non, en revanche, on y verra le moyen aisé du traçage d'autres délits bien plus mineurs et directement liés à l'utilisation des technologies de communication, ainsi la violation de droits d'auteur à propos d'œuvres présentes sur le Net, les tentatives de *hacking*, la fraude fiscale, etc. Mais que penser alors d'un discours qui agite le spectre terroriste pour en réalité atteindre une autre cible, celle des délits économiques, dont la recherche des auteurs n'apparaît pas justifier le recours aux moyens extraordinaires prévus. Ne faut-il pas en toute hypothèse –et la résolution du Parlement européen déjà évoquée en matière de lutte contre la pornographie enfantine y faisait déjà allusion– réserver à quelques infractions majeures le moyen évoqué ?

Les règles de proportionnalité, de nécessité, de prévisibilité et de légalité des mesures qui restreignent nos droits et libertés fondamentaux conduisent en toute hypothèse à exiger que la loi précise les limites strictes de la durée de conservation, qu'elle définisse les données d'identification concernées (les seules données de connexion de l'utilisateur et du moment de la "transaction" ne suffisent-elles pas ?[39]) et circonscrive à quelques prestataires de services obligés : ceux qui fournissent l'accès aux réseaux, le devoir de conservation. Il faudrait en particulier distinguer les mesures

38. Poussons le raisonnement à l'absurde. Tira-t-on du fait que les complices de Ben Laden –pour autant que celui-ci soit coupable– disposaient apparemment pour opérer l'attentat de lames de rasoir, la conséquence de la nécessité du fichage de tout individu achetant de telles lames ?

39. Il s'agit d'"exclure, dans la rédaction du décret, les données de communication pouvant être considérées comme des données indirectes de contenu ou de comportement". Certaines données techniques peuvent en effet fournir des éléments

policières ordonnées à propos de données qui sont déjà conservées par les opérateurs de télécoms et celles concernant les autres qui ne seraient conservées qu'à des fins policières.

Il est demandé donc au législateur d'agir ici comme ailleurs avec des "mains tremblantes" d'autant plus que les conséquences du prescrit en question engendrent des risques qu'on énumère ci-après.

Les risques de tels traitements

Le premier risque est celui de la dérive réglementaire : même avec les limites rappelées ci-dessus et clairement affirmées au départ, on craindra que la loi à peine votée ne voit progressivement son champ élargi et les garanties jugées trop "lourdes" abandonnées dans l'intérêt de l'efficacité. Depuis la première loi belge sur les repérages de communications, cinq autres lois ont suivi, élargissant chaque fois un peu les atteintes des autorités policières aux secrets des communications. Ainsi, dira-t-on demain, puisque de tels réservoirs de données existent, ne peut-on y recourir plus largement[40]. Cette tendance, une fois introduite une exception, à y en ajouter d'autres inquiète. Comment, sur ce point, ne pas louer la sagesse américaine du "*Patriot Act*" qui limite à l'horizon de quatre ans, les mesures exceptionnelles attentatoires aux libertés qui y sont contenues et d'ajouter que, parmi ces mesures, celle d'obliger à la conservation des données n'y est même pas reprise.

Parmi les premières réactions négatives à ces mesures les avocats ont souligné le danger que représentaient pour eux les atteintes ainsi facilitées au secret professionnel. L'autorité policière aura en effet quelques difficultés à démêler a priori parmi toutes les communications dont elle ordonnera le relevé, celles couvertes par le secret et les autres.

Ensuite, on rappellera que le renforcement de la cybersurveillance exige son contrôle par une autorité indépendante. Est-on sûr que le contrôle des investigations menées sur le terrain par des équipes policières bien entraînées sera effectif, que les autorités judiciaires ou spécifiques de

sur le contenu des informations transmises (par exemple, l'URL des sites visités, l'adresse IP du serveur consulté ou l'intitulé d'un courrier électronique), ou sur le comportement des internautes (adresse du destinataire d'un courrier électronique par exemple). Le Forum considère que ce type de données ne doit pas être mentionné dans le décret en préparation. En revanche, il considère que "l'adresse IP de l'utilisateur relève bien des données nécessaires à l'établissement de la communication et n'indique rien quant au contenu des informations consultées ou au comportement de l'internaute". Forum des droits sur l'Internet, Recommandations aux pouvoirs publics : conservation des données relatives à une communication électronique, 18 décembre 2001 disponible à http://www.foruminternet.org/recommandations/lire.phtml?id=230.

40. Ainsi, le débat en cours en France à propos de l'intérêt porté par l'administration fiscale aux données de connexion. Le Sénat a adopté le 18 décembre, dans le cadre du projet de loi de finances rectificative 2001, des amendements donnant accès pour les agents des douanes et les enquêteurs de la Commission des opérations de bourse (COB) aux données conservées par les fournisseurs d'accès et les opérateurs télécommunications au titre de la LSQ. Il en profite cependant pour proposer un nouvel amendement qui étend ce droit d'accès aux agents de l'administration fiscale.

contrôle pourront toujours saisir la portée des utilisations faites des moyens nouveaux d'investigation ? En outre, la circulation d'informations au sein des réseaux de collaboration internationaux ou européen n'exige-t-elle pas un renforcement des contrôles démocratiques ou juridictionnels d'Europol, d'Interpol, du futur "Eurojust" ou d'Enfopol ?

D'autres risques de dérive étaient déjà soulignés par la Commission belge de protection de la vie privée[41] lors du débat ayant mené au vote de la loi sur la criminalité informatique. La simple existence de tels fichiers crée en toute hypothèse des risques de dérive : les prestataires contraints à un tel stockage peuvent être tentés de rentabiliser leurs prestations à d'autres fins. Au-delà de la sécurisation de leurs propres services ou réseaux, on songe au profilage des utilisateurs à des fins propres ou de commercialisation. Certes on pourrait songer à confier la gestion de tels fichiers à des tiers spécialisés en conservation, *a fortiori* aux autorités policières, mais c'est substituer au risque décrit celui plus grand encore de fichiers mammouths où toutes les interconnexions deviennent possibles.

Si la Cour européenne des droits de l'Homme considère que le seul stockage de données à des fins policières est déjà une atteinte à nos libertés (Rotaru, Ammann...), les conséquences des traitements induits par les législations évoquées ci-dessus appellent des précautions bien plus importantes encore. En effet, on peut craindre que les forces de police ne puisent dans ces vastes réservoirs de données les premiers éléments de leurs enquêtes et ce, avant même toute autre investigation (repérage des personnes à proximité du lieu de commission de l'infraction, liste des correspondants, dernier appel entrant ou sortant...). Pis, elles peuvent être tentées d'y trouver les moyens d'une surveillance exploratoire de groupes dits "à risque", ceux qui furètent sur tel ou tel site, ceux qui se connectent au réseau à partir de tel ou tel endroit, jugé chaud, les présumés "terroristes" ou "*hackers*", etc.

Ainsi, il est absolument requis "d'interdire toute mise en place par les services de sécurité d'un accès général aux informations sauvegardées : l'interrogation des données conservées doit se faire dans le cadre d'une procédure précise, sur une base de requêtes au cas par cas. Il ne saurait être possible d'instaurer un accès permanent à ces données permettant la mise en place de traitements automatisés pouvant s'apparenter à une surveillance générale des réseaux. La conservation physique de ces données devra donc relever de la seule responsabilité des entreprises visées, qui devront en limiter strictement l'accès"[42].

41. Avis de la Commission belge de protection de la vie privée, déjà cité.

42. Forum des droits sur l'Internet, recommandations aux pouvoirs publics : conservation des données relatives à une communication électronique, 18. Décembre 2001, disponible à http://www.foruminternet.org/recommandations/lire.phtml?id=230. Sans doute, est-il à recommander également que la conservation tant par les fournisseurs et opérateurs que par les autorités policières s'opèrent avec des "logiciels libres" pour éviter que des manipulations puissent avoir lieu de manière non détectable par les autorités de contrôle.

Conclusions[43]

La lutte contre la cybercriminalité est affirmée comme une priorité sans laquelle nos sociétés ne pourraient survivre. Au nom de la sécurité, forts de l'opinion publique relayée et amplifiée par les médias, les pouvoirs politiques préparent dans la hâte, tant au niveau national qu'européen, des législations accroissant les pouvoirs des autorités judiciaires et policières afin de mener une lutte efficace contre la cyber-criminalité et le terrorisme. Osera-t-on leur rappeler que les bandes de Ben Laden, à supposer qu'elles soient coupables des événements du 11 septembre, ne semblent point avoir eu besoin des vertus d'Internet pour commettre leur crime et qu'Echelon n'a pas permis de déjouer leurs plans ?

Que disent ces législations écrites à la diable ? Elles obligent les divers fournisseurs de services de communications électroniques privées ou publiques –et ils sont nombreux– à conserver pendant un délai que d'aucuns estiment d'un an (notre législation belge fixe ce délai comme minimal !) les données qui résultent de notre utilisation de ces services et ce indépendamment d'une utilisation pour la fourniture de service de télécommunications. On génère des données sur toute la population pour les fins préventives de lutte contre la criminalité et ce sans soupçon concret.

Sans doute, objectera-t-on aux défenseurs des libertés que la liberté prônée est un luxe, alors même que certaines vies sont en danger. On ajoutera que l'homme honnête n'a rien à craindre de cette surveillance mieux assurée qui débusque les méchants et n'effraie pas le gentil. Certains iront jusqu'à évoquer le mérite de cette surveillance qui force à adopter un comportement toujours plus conforme aux normes sociales.

À ceux-là, qu'il me soit permis de répondre. Il n'est selon moi pire danger que cette cybersurveillance qui traque l'homme dans son intimité et crée chez lui la hantise perpétuelle du dévoilement. "Par un renversement pervers, cette prééminence obsessionnelle du regard de l'autorité se fait au nom même de ce qu'elle détruit. Les valeurs derrière lesquelles elle s'abrite sont de haut vol : justice, liberté, démocratie, respect des lois, civisme, intégrité. Mais qui ne voit que derrière cette vision, décapante parfois à force d'user les cibles sur lesquelles elle porte, lime jusqu'à l'os certains principes qui fondent le vouloir vivre ensemble ? Quand la proportionnalité n'est plus respectée entre les moyens que se donne l'investigation et les buts recherchés, la sacralisation de l'investigation et du dévoilement assoit comme légitimité unique le moyen et non plus la cause".

De plus, de telles mesures qui créent artificiellement un sentiment de sécurité évitent que ceux qui les prennent s'interrogent sur le pourquoi du crime et les instruments de politique criminelle qui permettent de faire face à cette montée de violence. Tout passe par la criminalisation et la

43. Nos conclusions reprennent certains passages de l'exposé de l'auteur lors de l'audition organisée par la Commission européenne à Bruxelles le 27 novembre 2001, audition relative à la lutte contre la cybercriminalité. L'intervention a été publiée *in extenso* sous le titre "Sécurité ou Libertés ?", Ubiquité, *Revue de droit des technologies de l'information*, Larcier, Bruxelles, 2002, p. 3 et s.

défense de la société sans interrogation supplémentaire. Or, on le sait, la criminalité finit toujours par se déplacer ou devenir plus violente si on ne s'attaque pas réellement à ses causes.

■

Bibliographie

Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social et au Comité des Régions : "Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité", Bruxelles, COM(2000)890 final.

COSTES L., "La convention du Conseil de l'Europe du 8 novembre 2001 : premier traité international contre la *cybercriminalité*", Lamy, *Cahiers droit de l'informatique*, n° 142, décembre 2001.

DE SCHUTTER B. et POULLET Y. (rapporteurs), avis n° 33/99 du 13 décembre 1999 relatif aux projets de loi relatifs à la criminalité informatique, avis disponible sur le site de la Commission belge de protection de la vie privée : http://www.privacy.fgov.be, et publié dans les documents parlementaires de la Chambre des représentants (Doc. Parl. Chambre, 0213/004). On notera que cet avis a été pris à l'initiative de la Commission, celle-ci n'ayant pas été consultée par le Gouvernement. *Cf.* également, l'avis très critique du Conseil d'État, publié in Doc.Parl. 213/002).

DE VILLENFAGNE Fl. et DUSOLLIER S., *La Belgique sort enfin ses armes contre la cybercriminalité*, Auteurs et Médias, 2001, p. 77 et s. ;

DINANT J.-M., rapport rédigé pour le projet européen ECLIP, disponible à http://www.droit.fundp.ac.be/textes/privacy_law_tech_convergence.rtf.

FRAPPAT B., "La dictature de la transparence", *Études*, 1999, p. 58.

GNING E.M., "Le projet de convention sur la criminalité dans le cybersespace", *Lex Electronica*, vol. 6, n° 2, 2001, disponible à http://www.lex-electronica.org/articles/v6-2/gning.htm.

HAVELANGE B. et POULLET Y., "Secret d'État et vie privée ou comment concilier l'inconciliable ?", Colloque international du 20 janvier 1999 organisé par le Comité R., in Droit des technologies de l'information et de la communication, *Cahier du Crid*, n° 16, BRUYLANT, 1999.

MEUNIER C., "La loi du 28 novembre 2000 relative à la criminalité informatique", *Actualités du droit des technologies de l'information et de la communication*, CUP, vol. 45, février 2001.

OST F., "Le concept de "démocratie" dans la jurisprudence de la Cour européenne des droits de l'Homme", *Journal des Procès*, n° 124, 1998.

POULLET Y., DINANT J.-M., "Le réseau Echelon, existe-t-il ? Que peut-il faire ? Peut-on et doit-on s'en protéger ?", Rapport d'expertise rédigé à l'attention du Comité permanent de contrôle des services de renseignements, mai 2000, disponible à http://www.crid.ac.be/.

POULLET Y., LOUVEAUX S. et PEREZ-ASINARI M.-V., "Data Protection and privacy in Global Networks : An European Approach", *EDI Law Review*, 2001.

POULLET Y., "À propos du projet de loi dit n° 214 : la lutte contre la cybercriminalité dans le cyberespace à l'épreuve du principe de la régularité des preuves", in *Liber amicorum*, DU JARDIN J., VUYE H. et POULLET Y., éd., Kluwer, 2001.

VAN EECKE P., *Criminaliteit in Cyberspace*, Mijs en Breesch, Gent, 1997.

VAN EECKE P., "Het voorontwerp van wet inzake informaticacriminaliteit", in *Recente ontwikkelingen in informatica en telecommunicatie recht*, ICRI, Die Keure, Brugge, 1999.

YERNAULT D., "De la fiction à la réalité : le programme d'espionnage électronique global "Echelon" et la responsabilité internationale des États au regard de la convention européenne des droits de l'Homme", *Revue belge de droit international*, 2000.